CPTC Procedure: Computer and System Logging

Overview
Computer logs are essential to the operational management of an organization. They provide a primary mechanism for automated tracking and reporting for review, audit, and compliance functions as well as a useful mechanism for tracking changes and troubleshooting.

Purpose
The purpose of this procedure is to provide accurate and reliable audit logs in order to detect and react to inappropriate access to, or use of, computing or network systems or data. This can be summed up by the following three goals.

1. Access to networking and computing systems and data as well as significant system events must be logged by the Information System.
2. Information System audit logs must be protected from unauthorized access, modification, or destruction.
3. Information System audit logs must be retained for an appropriate period of time, based on the Document Retention Schedule and business requirements. Current TCSG guidelines require that logs to critical assets be kept at least 3 months with a preferred 12 month retention period.

This document will provide logging procedures designed to establish a baseline for components across the Coastal Pines Technical College Network (CPTC). This document is designed to augment logging guidelines spelled out by TCSG in their documentation. Further, this procedure is a derivative of a section of the TCSG Security Guidelines. Any changes or differences in the TCSG document will supersede the CPTC procedure.

Scope
This procedure applies to all Coastal Pines Technical College staff that create, deploy, or support application and system software. Though it largely pertains to the IT department, it may apply to other system and data owners in the College or that support CPTC systems or data.

General
Significant events generated by Coastal Pines Technical College's network, systems and communications devices shall be logged and monitored to identify suspicious activity or system health events that may indicate potential misuse as well as health or reliability issues with the devices or systems. Log servers and documents shall be kept secure and only made available to personnel authorized by the CPTC Information Security Administrator (ISA) or designee. The ISA is appointed by the Technical College of Georgia (TCSG) for each college in the system. Authorized personnel or SIEM software will analyze the logs for significant events.

Coastal Pines Technical College's critical network infrastructure such as servers, workstations, firewalls, routers, switches, and communications equipment shall be monitored and logged in order to:

- Ensure use is authorized
- Manage, administer, and troubleshoot systems
- Detect unauthorized access or access attempts
- Detect and prevent criminal or illegal activities
- Provide a basis for forensic investigations

- Provide a record of baseline traffic
- Comply with TCSG's policies and procedures

Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain sufficient audit logging information to enable IT personnel to Determine:

- The activity that was performed.
- Who or what performed the activity.
- Systems, devices, or objects involved.
- When the activity was performed.
- Status, outcome, and/or result of the activity (such as success vs. failure)

Coastal Pines Technical College shall implement a suitable logging infrastructure and configure all critical devices, systems, and applications with logged audit trails. The ISA or designee shall ensure important events and audit trails are logged. All logs must be stored on separate devices, preferably a SYSLOG or SIEM server.

Logged Events

The system events and activities below shall be monitored and logged at a minimum:

- System administrator and system operator activities.
- System start-ups and shut-downs.
- Exceptions and security events.
- All firewalls and core switches with ACLs or policy on them.
- Intrusion Prevention Systems (IPS).
- Authentication successes and failures (e.g. log in, log out, failed logins).
- User security authorizations.
- Any login and file access attempts to Banner RDBMS servers. (Per TCSG, these must be enabled with logs stored on separate logging hosts. The minimum storage period is 90 days.)
- Granting, modifying, or revoking access rights to include new user or group additions, user privilege modifications, file or database object permissions, firewall rules, and user password changes.
- Accessing the Internet. All internet activity is logged, monitored, and subject to review and publication.
- Accessing the College VPN. All VPN access to the Campus LAN must be logged.

Logging Event Contents

Log entries can contain a number of elements based on the type and function of the system or process being audited. Unless otherwise required, logging events shall include the following information where applicable:

- Hostname/IP address (system identification)
- Peer host name/IP Address (remote system identification)
- Date/Time Stamp
- Application ID (e.g. name and version)
- The event ID or action and any relevant data where feasible or within the logging level
- User ID causing/associated with event
- Event type
- Success or failure of the action

- Resource (e.g. identity or name of affected data, component)
- Logging level/Severity of event (e.g. critical, error, alert, warning, information only, 0-7)

Log Aggregation and Storage

The logging system shall support the following features to ensure integrity and support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following approaches:

- Collecting Microsoft Windows Event Logs from servers by a centralized logging management system
- Storing logs in a documented format and sent via reliable network protocols to a centralized SYSLOG or SIEM system

System Reports of Information Not Sent to Centralized Logs

Some critical systems do not send important reports to centralized logging servers but do send out periodic reports that affect the security, data protection, and reliability of mission critical components. These reports should be read and analyzed in the shortest period feasible based on how bad information can adversely affect the security and reliability of the systems. The responsibility for initiating remediation measures or creating a ticket will be on the system owner, manager, or primary administrator. If that person is unavailable, the backup admin for that device or system will monitor the reports and initiate remediation.

Information Security Issues

Since logging is one of the most fundamental tools used by system administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems, careful measures shall be taken to ensure the confidentiality, availability and integrity of all logs and logging systems. These measures shall include:

- Protection of the system logs and their contents from unauthorized access, modification, and/or deletion.
- Limiting the ability of administrators and those with elevated access to disable, damage, or circumvent access control and audit log mechanisms.
- Limiting outside access to logging systems to authorized access. Any emergency access should be authorized by the TCSG ISO or CIO if the CPTC ISA is not available.
- Limiting changes to the auditing rules and policies to stop logging of an unauthorized activity.
- Configuring log settings to track and record user policy changes.

Administrative Responsibilities

The CPTC ISA or designee shall be responsible for items in the list below.

- Separating duties between operations and security monitoring when applicable and feasible.
- Ensuring a regular review and analysis of activity audit logs.
- Establishing logging levels of critical devices and systems.
- Securing audit trails by limiting viewing to those with a need to know.
- Protecting audit trail files from unauthorized modifications.
- Ensuring audit logs and log files are promptly backed up to a centralized log server or media.
- Preserving evidence from any potential incidents per the CPTC Incident Response Plan.
- Review logging for performance delays
- Verify access to log files is properly restricted

- Assist with investigations
- Determine when the data center has been entered and by whom. Physical access to the data center must be limited to authorized personnel and logged, either electronically or manually.
- Configure and ensure debug level logging on all firewalls.
- Provide, at a minimum, 90-day retention periods for all critical logs. One-year retention is desirable if feasible.

Executive Directors of IT, IT Supervisors, and Information System Administrators (ISAs) are responsible for developing and implementing procedures for the reporting of inappropriate or unusual activity as well as monitoring and reviewing audit logs to identify and respond to inappropriate or unusual activity. Other IT staff may be assigned to review and monitor the logs for systems for which they are the primary or backup administrator. Logs shall be reviewed on a regular and on-going basis. The frequency of review shall be determined according to the sensitivity of the information stored, the function of the system, and other system requirements as determined by the system administrator and/or TCSG. The CPTC ISA will determine whether to escalate potential security incidents to the TCSG ISO for analysis based on the guidelines in the CPTC Security Incident Response Plan as well as the TCSG Information Security Standards.

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Coastal Pines Technical College procedures. Examples of auditable controls include:

- On demand and historical log reviews of areas described in this policy.
- Documented communications surrounding logging activities.
- Incident response procedures.
- Logging infrastructure will be monitored by a centralized monitoring server (PRTG) to ensure that the syslog server is accessible and the drives have adequate storage capacity.

Penalties:

Violations of these procedures incur the same types of disciplinary measures as violations of other CPTC policies or state or federal laws, including criminal prosecution.

Responsibility

The Executive Director of Information Technology has the overall responsibility for ensuring this procedure is implemented.

Adopted: January 12, 2021
Revised: September 19, 2023